AlienVault를 ESA의 외부 위협 피드로 구성

목차

소개

이 문서에서는 AlienVault 소스에서 외부 위협 피드를 구성하고 ESA 내에서 이를 사용하는 단계를 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Cisco SEG/ESA(Secure Email Gateway) AsyncOS 16.0.2

- Linux CLI
- Python3 pip
- AlienVault 계정

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Email Security Appliance
- 파이썬3

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

ETF(External Threat Feeds) 프레임워크를 사용하면 이메일 게이트웨이가 TAXII 프로토콜을 통해 STIX 형식으로 공유된 외부 위협 정보를 수집할 수 있습니다. 조직은 이 기능을 활용하여 다음을 수행할 수 있습니다.

- 악성코드, 랜섬웨어, 피싱, 표적 공격과 같은 사이버 위협에 대해 사전 대응적인 입장을 취합니다.
- 로컬 및 서드파티 위협 인텔리전스 소스를 모두 구독합니다.
- 이메일 게이트웨이의 전반적인 효과를 향상시킵니다.

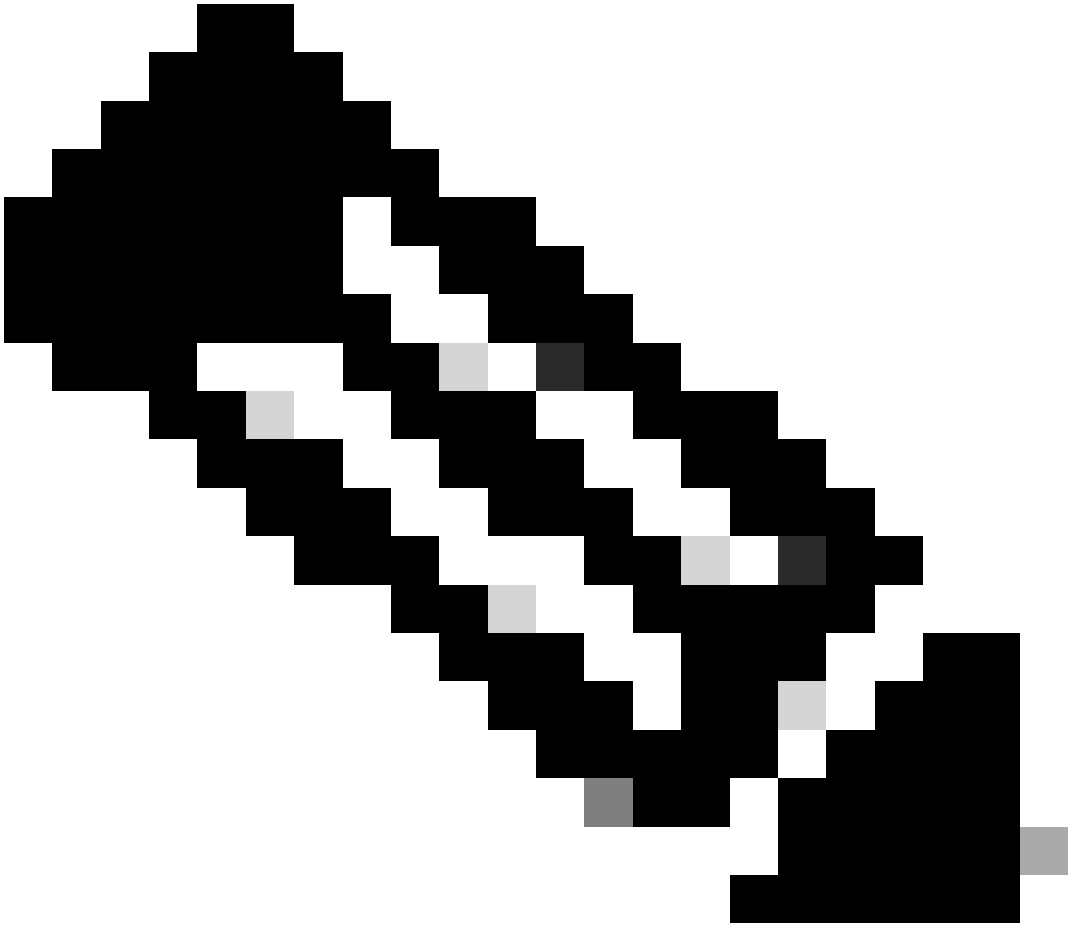
STIX/TAXII란 무엇입니까?

STIX(구조적 위협 정보 표현)

STIX는 지표, 전술, 기법, 악성코드, 위협 행위자를 포함하여 CTI(Cyber Threat Intelligence)를 체계적이고 기계 판독이 가능한 방식으로 설명하는 데 사용되는 표준화된 형식입니다. STIX 피드에는 일반적으로 의심스럽거나 악의적인 사이버 활동을 탐지하는 데 도움이 되는 지표인 패턴이 포함됩니다.

TAXII(신뢰할 수 있는 자동화된 인텔리전스 정보 교환)

TAXII는 시스템 간에 STIX 데이터를 안전하고 자동으로 교환하는 데 사용되는 프로토콜입니다. 전용 서비스(TAXII 서버)를 통해 시스템, 제품 또는 조직 간에 사이버 위협 인텔리전스를 교환하는 방법을 정의합니다.



참고: AsyncOS 16.0 릴리스는 STIX/TAXII 버전을 지원합니다. STIX 1.1.1 및 1.2, TAXII 1.1 포함

피드 소스

Email Security Appliance는 공용 저장소, 상용 공급자, 조직 내 자체 프라이빗 서버 등 다양한 소스의 위협 인텔리전스 피드를 사용할 수 있습니다.

호환성을 보장하려면 모든 소스에서 STIX/TAXII 표준을 사용해야 하며, 이를 통해 체계적이고 자동화된 위협 데이터 공유가 가능합니다.

카보비 도서관

Cabby Python 라이브러리는 TAXII 서버에 연결하고 STIX 컬렉션을 검색하고 위협 데이터를 폴링

하는 데 유용한 툴입니다. Email Security Appliance에 통합하기 전에 피드 소스가 제대로 작동하는지, 그리고 예상대로 데이터를 반환하는지 테스트하고 검증하는 좋은 방법입니다.

Cabby 라이브러리 설치

Cabby 라이브러리를 설치하려면 로컬 컴퓨터에 Python pip가 설치되어 있는지 확인해야 합니다.

python pip를 설치한 후에는 이 명령을 실행하여 cabby 라이브러리를 설치하면 됩니다.

```
python3 -m pip install cabby
```

cabby 라이브러리 설치가 완료되면 taxii-collections 및 taxii-poll 명령을 사용할 수 있는지 확인할 수 있습니다.

```
(cabby) bash-3.2$ taxii-collections -h
usage: taxii-collections [-h] [--host HOST] [--port PORT] [--discovery DISCOVERY] [--path URI] [--https
                         [--cert CERT] [--key KEY] [--key-password KEY_PASSWORD] [--username USERNAME]
                         [--proxy-url PROXY_URL] [--proxy-type {http,https}] [--header HEADERS] [-v] [-
```

```
(cabby) bash-3.2$ taxii-poll -h
usage: taxii-poll [-h] [--host HOST] [--port PORT] [--discovery DISCOVERY] [--path URI] [--https] [--ve
                  [--key KEY] [--key-password KEY_PASSWORD] [--username USERNAME] [--password PASSWORD]
                  [--proxy-type {http,https}] [--header HEADERS] [-v] [-x] [-t {1.0,1.1}] -c COLLECTION
                  [-b BINDINGS] [-s SUBSCRIPTION_ID] [--count-only]
```

AlienVault - 펄스 및 피드

AlienVault 정보 검색을 시작하려면 먼저 AlienVault 사이트에 계정을 만든 다음 원하는 정보 검색을 시작합니다.

AlienVault에서 피드와 펄스는 서로 관련되지만 동일하지는 않습니다.

펄스

펄스는 그룹화된 지표 + 상황(사람이 읽을 수 있음)을 포함하는 위협 인텔리전스입니다.

- Pulse는 특정 위협 또는 캠페인을 중심으로 그룹화된 위협 지표(IOC)의 모음입니다.
- 악성코드, 피싱, 랜섬웨어 등을 설명하기 위해 커뮤니티 또는 제공자에 의해 생성됩니다.
- 각 펄스에는 위협 설명, 관련 표시기(IP, 도메인, 파일 해시 등), 태그 및 참조와 같은 컨텍스트가 포함됩니다.
- 펄스는 사람이 쉽게 이해하고 공유할 수 있는 방식으로 판독 가능하고 구조화된다.

펄스를 그룹화된 IOC 및 메타데이터가 있는 위협 보고서로 간주합니다.

피드

피드는 다중 펄스(기계 판독 가능)로부터 지시자의 자동화된 스트림이다.

- 피드는 하나 이상의 펄스로부터 끌어오는 원시 표시기(IOC)의 스트림이며, 대개 자동화된 방식으로 이루어집니다.
- 일반적으로 보안 툴에서 STIX/TAXII, CSV 또는 JSON 등의 형식을 통해 대량으로 지표를 수집하는 데 사용됩니다.
- 피드는 기계에 초점을 맞추고 자동화와 SIEM, 방화벽, 이메일 게이트웨이와의 통합에 사용됩니다.

피드는 전달 메커니즘에 대한 것이며, 펄스는 위협의 내용과 컨텍스트입니다.

일반적으로 피드를 폴링하며, 이러한 피드는 펄스에서 추출된 표시기로 구성됩니다.

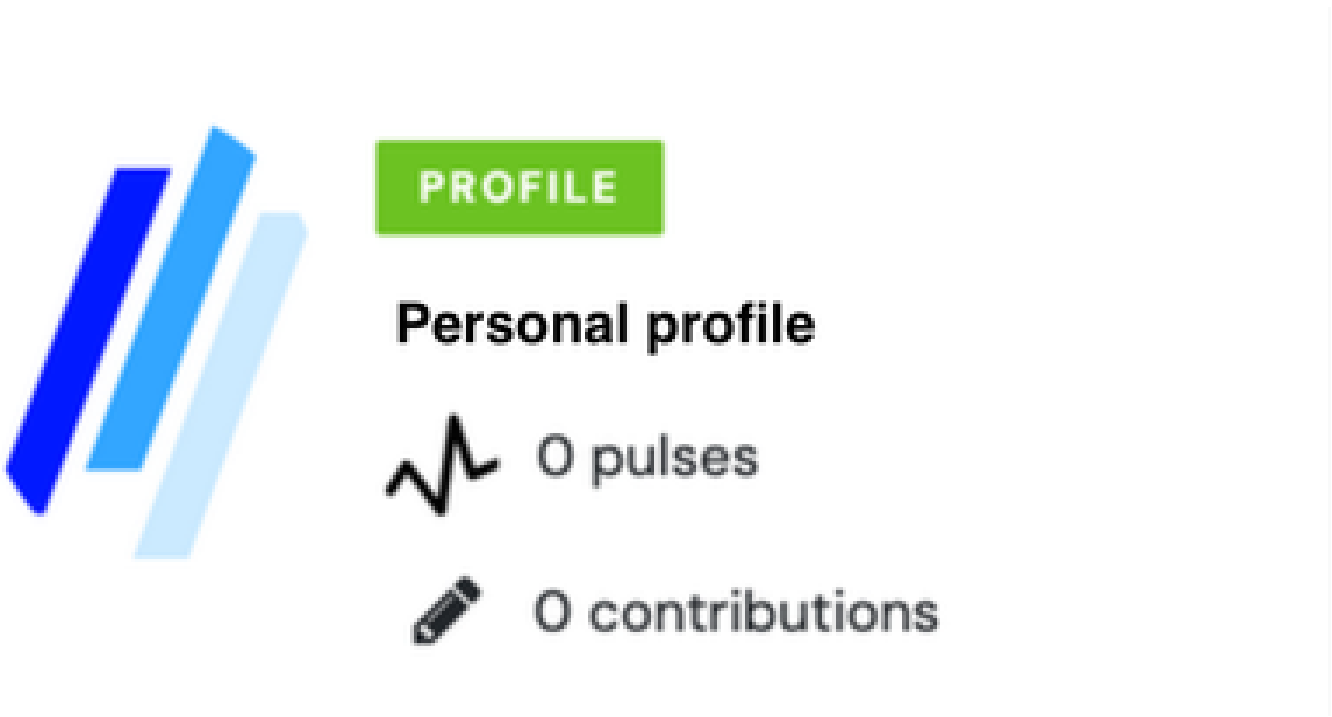
컬렉션 폴링 시작

자체 프로필에서 폴링

AlienVault 계정을 갖게 되면 taxii-collections 및 taxii-poll 명령을 사용할 수 있습니다.

이 활용 사례에서 다음 명령을 사용하는 방법은 다음과 같습니다.

이 경우 AlienVault 프로필 내에는 사용 가능한 펄스가 없지만 테스트로 taxii-poll 명령을 사용하여 프로필에서 컬렉션을 폴링할 수 있습니다.



alienvault 개인 프로필

```
taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_

        --username abcdefg --password ****
```

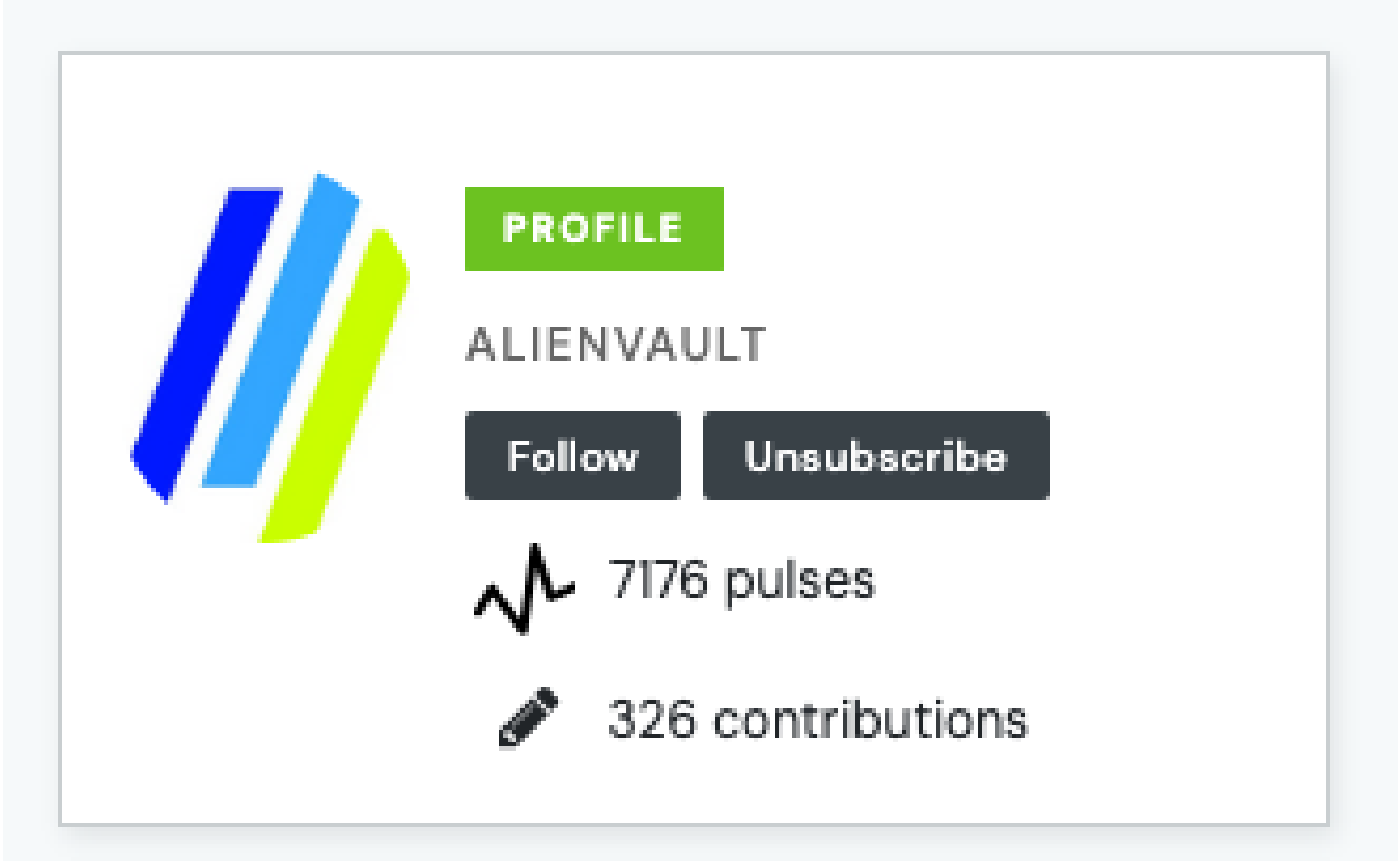
```
(cabby) bash-3.2$ taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_diegoher\
>     --username                                                          --password
2025-05-27 12:13:40,642 INFO: Polling using data binding: ALL
2025-05-27 12:13:40,643 INFO: Sending Poll_Request to https://otx.alienvault.com/taxii/poll
2025-05-27 12:13:41,51 INFO: 0 blocks polled
```

설문 개인 프로필

보시다시피 AlienVault 프로필 내에서 사용할 수 있는 정보가 없으므로 폴링되는 블록이 없습니다.

AlienVault 프로파일에서 폴링

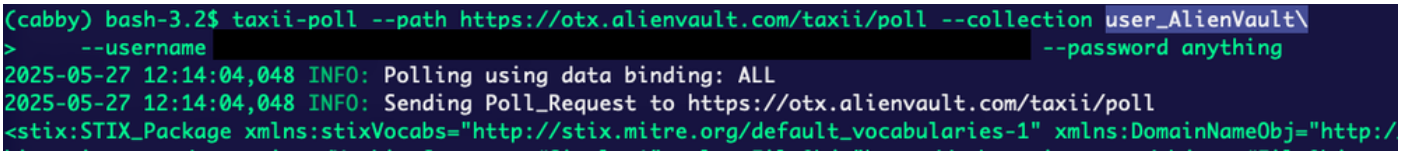
AlienVault 내의 프로파일이 발견되면 일부 프로파일에는 펄스가 있습니다. 이 예에서는 AlienVault 프로파일이 사용됩니다.



alienvault 프로필

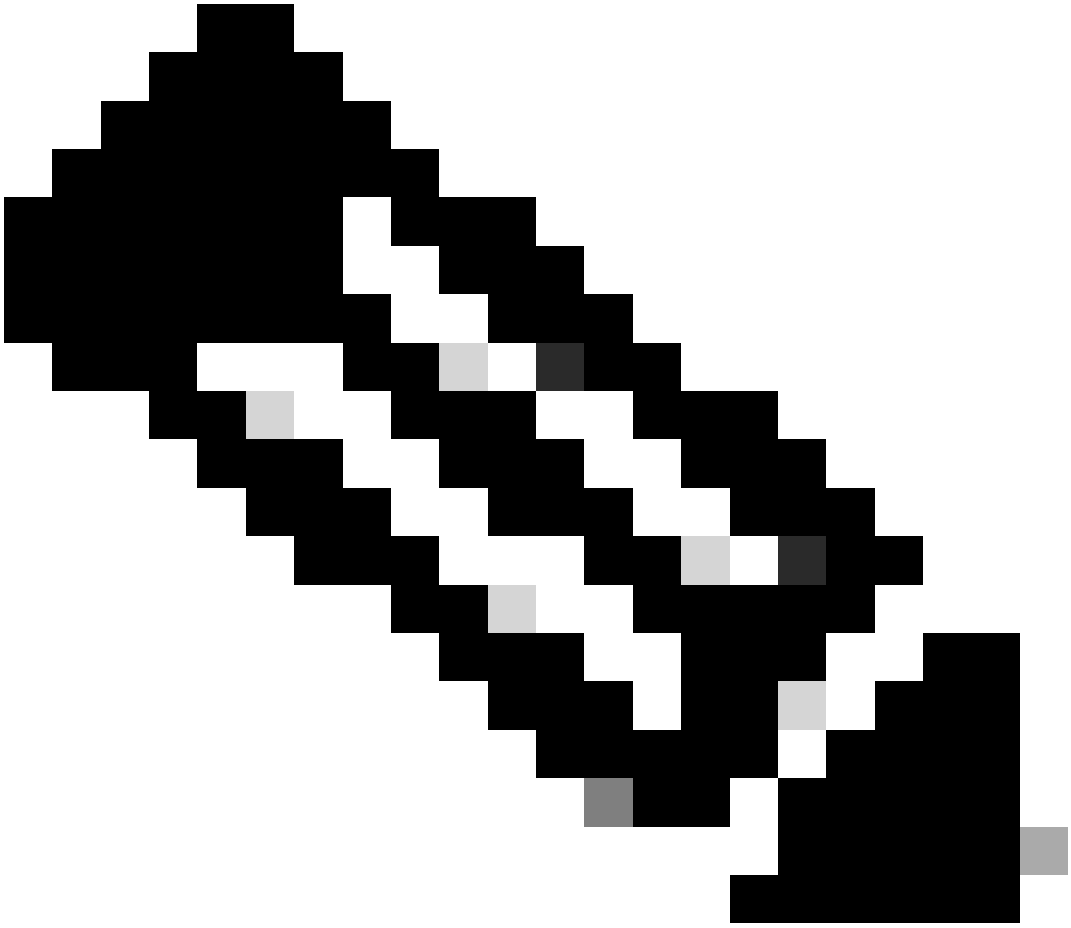
taxii-poll 명령으로 폴링을 실행하면 프로필에서 모든 정보 가져오기가 즉시 시작됩니다.

```
taxii-poll --path https://otx.alienvault.com/taxii/poll --collection user_AlienVault --username abcdefg
```



alienvault 설문조사

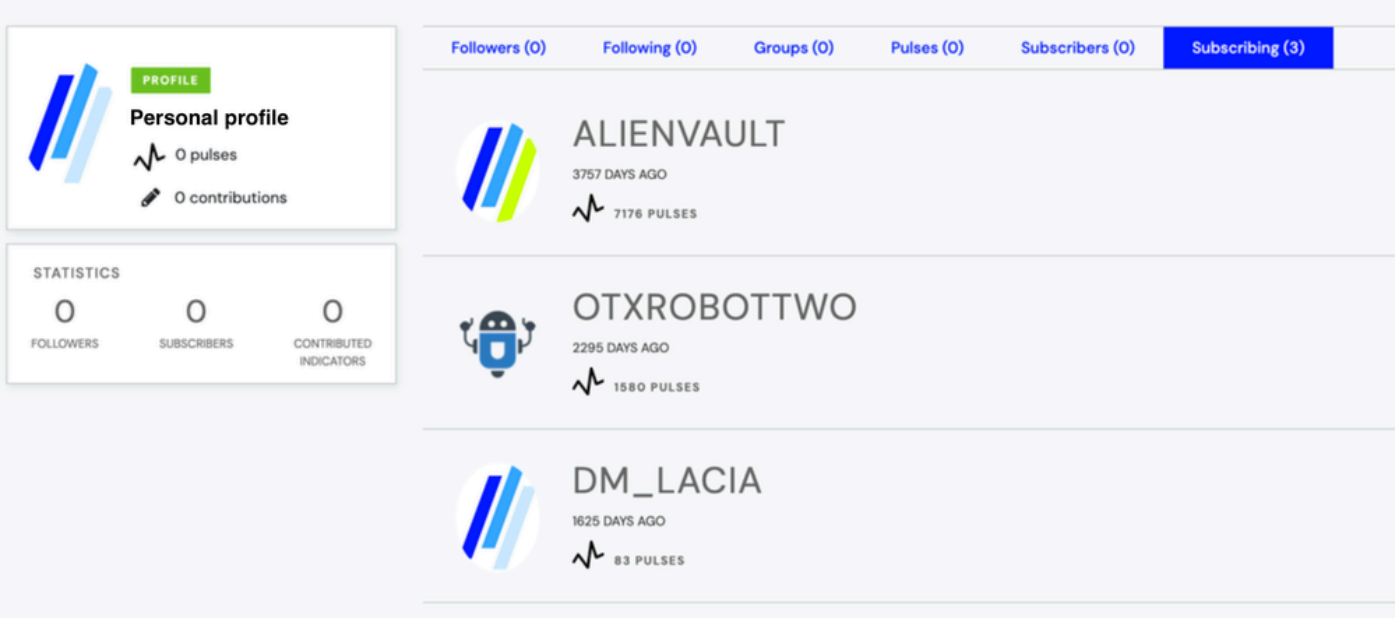
그림과 같이, 프로세스는 정보 가져오기를 시작합니다.



참고: 사용자 이름과 비밀번호를 확인하려면 다음 링크를 확인하십시오. https://otx.alienvault.com/api

AlienVault 프로필 컬렉션 구독

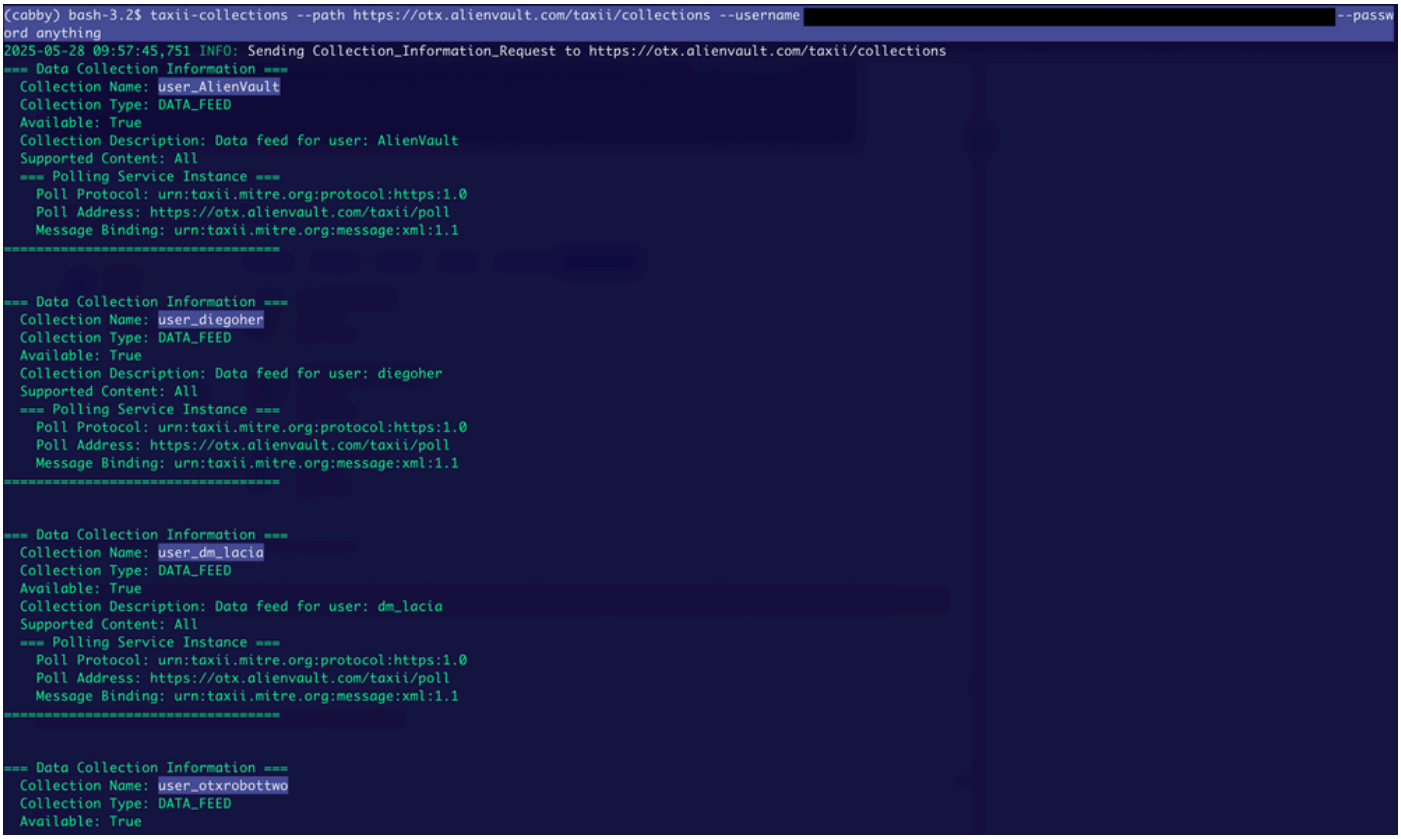
이 사용자는 테스트로 3개의 프로필을 구독했습니다.



개인 프로필 구독

taxii-collections 명령을 사용하여 서브스크립션을 가져올 수 있습니다.

```
taxii-collections --path https://otx.alienvault.com/taxii/collections --username abcdefg --password ***
```



개인 프로필 수집

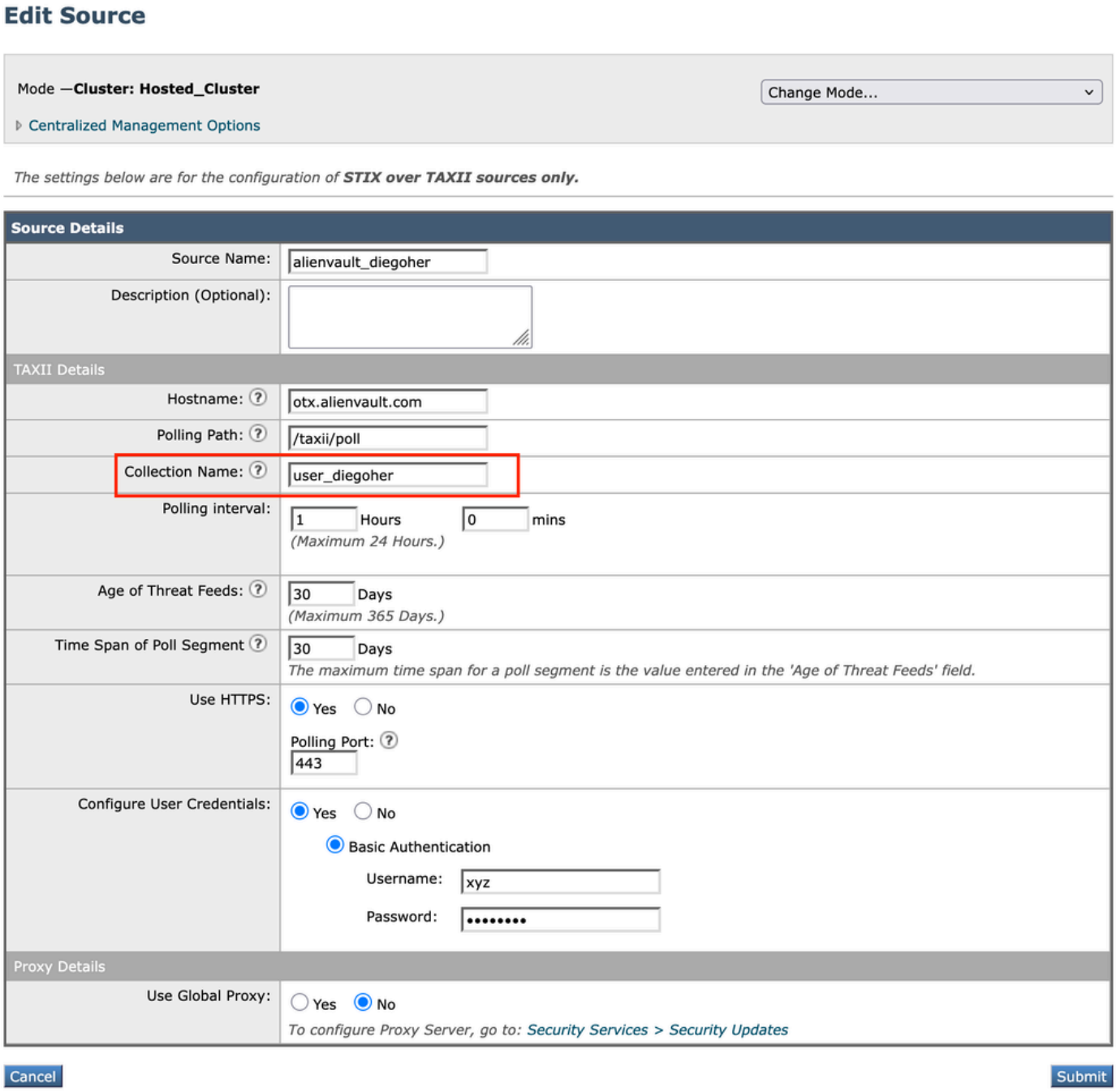
Collection Name(컬렉션 이름)이 가입한 이름과 동일한 경우 taxii-collections 명령이 작동하는지 확

인할 수 있습니다.

ESA에 소스 추가

피드 없이 소스 추가

1. Mail Policies(메일 정책) > External Threat Feeds Manager(외부 위협 피드 관리자)로 이동합니다.
2. 클러스터 모드로 변경합니다.
3. Add Source(소스 추가)를 클릭합니다.
4. 호스트 이름: otx.alienvault.com
5. 폴링 경로: /taxi/poll
6. 컬렉션 이름: user_<your_AlienVault_username>
7. 포트: 443
8. 사용자 자격 증명을 구성합니다. AlienVault에서 제공하는 서비스입니다.
9. Submit(제출) > Commit Changes(변경 사항 커밋)를 클릭합니다.



개인 정보

피드 없는 폴링 소스

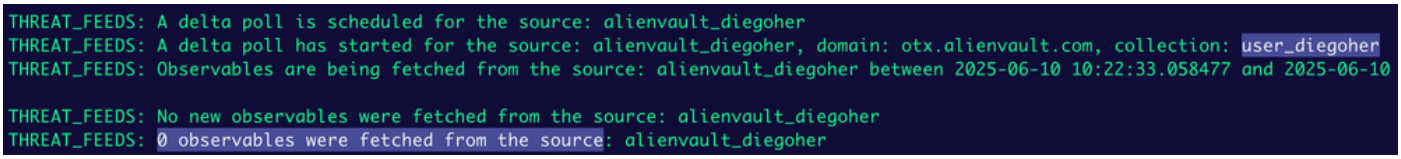
외부 위협 피드 관리자에서 소스가 추가되면 새로 추가된 소스가 표시됩니다.

개인 피드

추가한 후 Poll Now(지금 폴링)를 클릭합니다.

다음을 확인합니다.

CLI를 통해 ESA에 로그인하고 threatfeed 로그를 검토하여 정보를 확인합니다.

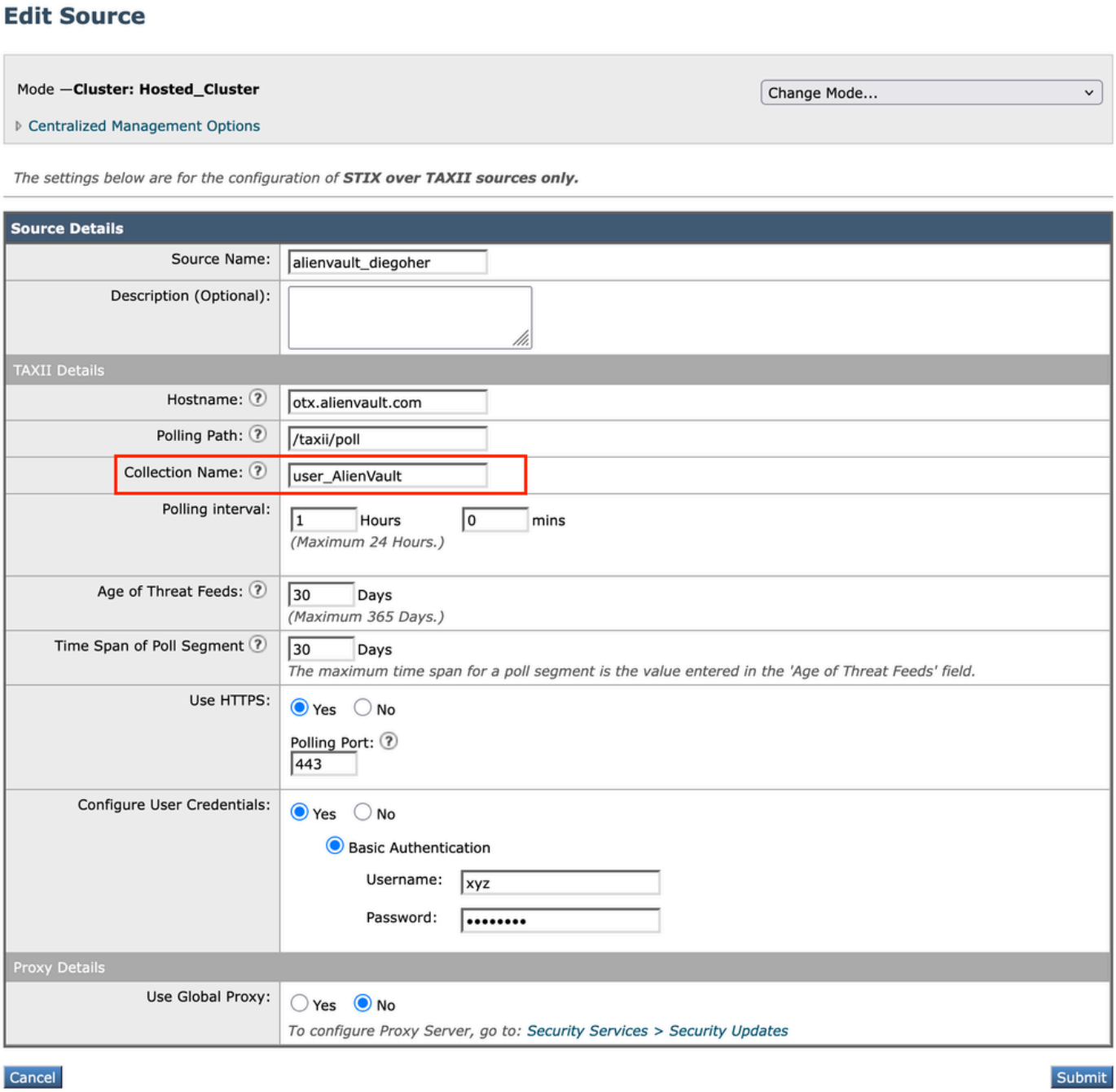


ETF 개인 설문조사

그림에서 볼 수 있듯이 관찰 가능한 0개를 가져왔으며 이는 표시된 프로파일에 피드가 없기 때문에 예상된 것입니다.

피드를 사용하여 소스 추가

1. Mail Policies(메일 정책) > External Threat Feeds Manager(외부 위협 피드 관리자)로 이동합니다.
2. 클러스터 모드로 변경합니다.
3. Add Source(소스 추가)를 클릭합니다.
4. 호스트 이름: otx.alienvault.com
5. 폴링 경로: /taxi/poll
6. 컬렉션 이름: 사용자_AlienVault
7. 포트: 443
8. 사용자 자격 증명을 구성합니다. AlienVault에서 제공하는 서비스입니다.
9. Submit(제출) > Commit Changes(변경 사항 커밋)를 클릭합니다.



alienvault 소스

피드가 있는 폴링 소스

외부 위협 피드 관리자에서 소스가 추가되면 새로 추가된 소스가 표시됩니다.

alienvault 피드

추가한 후 Poll Now(지금 폴링)를 클릭합니다.

다음을 확인합니다.

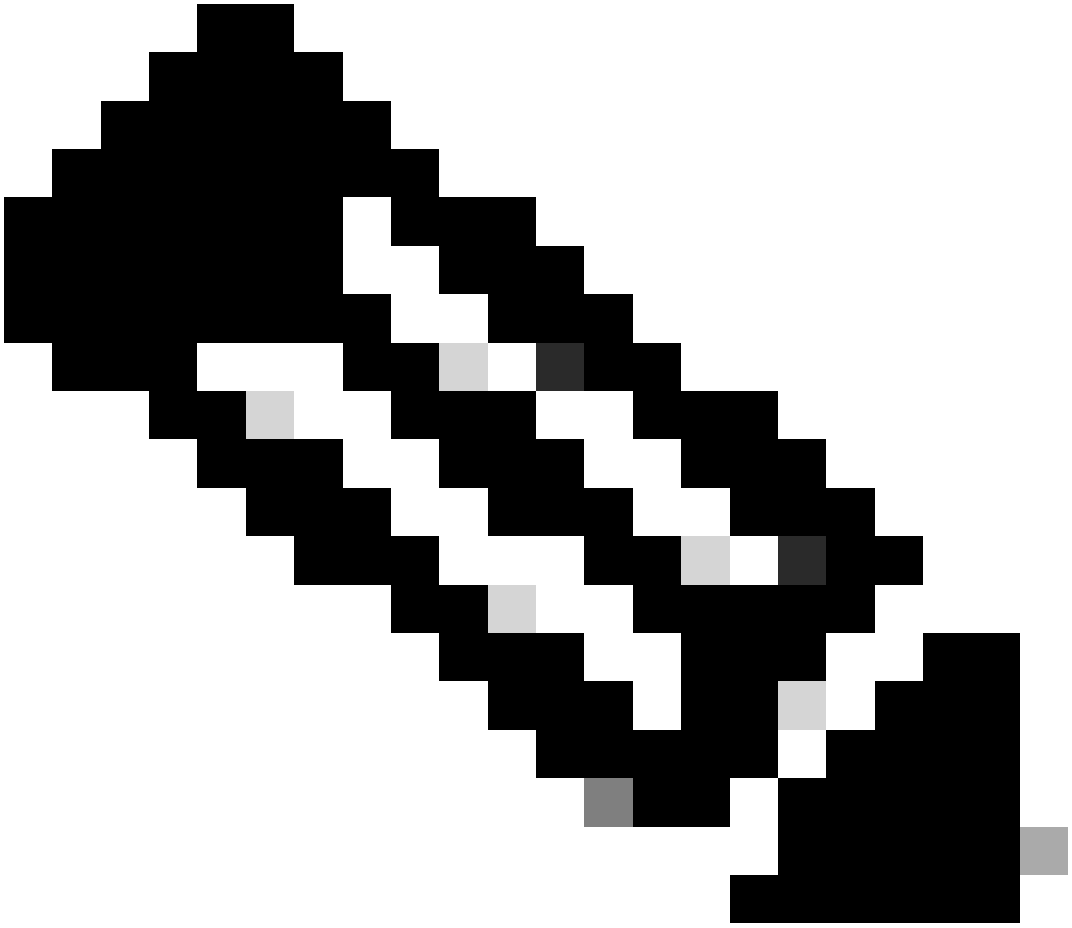
CLI를 통해 ESA에 로그인하고 threatfeed 로그를 검토하여 정보를 확인합니다.

```
THREAT_FEEDS: A full poll has started for the source: alienvault_diegoher, domain: otx.alienvault.com, collection: user_AlienVault
THREAT_FEEDS: All feeds from the source: alienvault_diegoher has been purged successfully.
THREAT_FEEDS: Observables are being fetched from the source: alienvault_diegoher between 2025-05-11 12:43:56.235896 and 2025-06-10

THREAT_FEEDS: The external threat feeds engine has started
THREAT_FEEDS: 6757 observables were fetched from the source: alienvault_diegoher
```

폴링 alienvault 피드

그림에서 볼 수 있듯이 여러 개의 관찰 가능성들을 가져왔다는 것을 알 수 있다.



참고: 구성된 컬렉션에 새 피드가 추가되면 ESA는 자동으로 소스를 폴링하고 새 관찰 가능 요소를 가져옵니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.